PHT
firsthand knowledge™

January 3, 2005

Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers lane, Rm 1061
Rockville, Md. 20852

Re: Docket # 2004D – 0440, *Computerized Systems Used in Clinical Trials*

Dear Sir or Ms.,

We are submitting the enclosed comments to the Referenced Docket number and Draft Guidance on behalf of PHT Corporation located at 500 Rutherford Avenue, Charlestown, Massachusetts 02129.

To simplify our comments, we have made them directly on the enclosed draft guidance copy. This letter also lists and summarizes them as follows:

Table of Comments.

Lines 95 – 96: Comment regarding "electronic record".

Line 107: This is a misspelled word – "trials" not "trails" should be used.

Lines 137 – 147: Wording recommendation and commentary regarding SOPs.

Line 156: Additional working regarding tokens and keys.

Lines 163 – 166: We believe there are other means of controlling access other than the ever changing "password," and hope that this document will provide for some of these alternatives such as those described in our comments on the document.

Lines 307 – 309: Comment regarding patient privacy in the context of recording access rights and privileges.

Line 329: Recommend adding "investigator", as shown in the text.

Lines 350 – 351: We believe that documentation should be available that demonstrates the entire computer system not just software for purposes of validation. To that purpose, we recommend removing the phrase, "regulated company" and changing "demonstrates software validation" to, "demonstrates computer system validation".

PHT
firsthand knowledge™

Line 375: “Off the shelf Software” should be defined.

Lines 394 – 405: We believe that some editorial clarification would be helpful, and have suggested some language for that purpose.

Lines 507 – 519: Comment regarding potential impact of registering the intent to use e-signatures in those cases where patients might be using electronic signatures to sign records.

Lines 533 – 535: Comment regarding potential conflict between the need for data attributability *vs*. the need for patient privacy.

Line 559: Added a suggested definition for “eSource” along with some comments on certified copies.

Lines 560 – 563: Comment regarding the meanings of “original data” and “first recording of study data”.

We hope that these suggestions and comments will be helpful.

Sincerely,

Stephen A. Raymond, Chief Scientific Office
Richard J. LaFleur, Director of QA and Compliance
Gerald F. Meyer, Regulatory Affairs Consultant

Guidance for Industry
Computerized Systems Used in Clinical Trials

DRAFT GUIDANCE — ERRATUM

On line 563 of this draft guidance, reference is made to Compliance Policy Guide (CPG) # 7130.13. This is incorrect. The CPG number should be 7150.13.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)

September 2004
Compliance

Revision 1

Guidance for Industry
Computerized Systems Used in Clinical Trials

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Comments and suggestions regarding this draft document should be submitted within 90 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit comments to the Division of Dockets Management (HFA-305), Food and Drug Administration, 5630 Fishers Lane, rm. 1061, Rockville, MD 20852. All comments should be identified with the docket number listed in the notice of availability that publishes in the *Federal Register*.

For questions regarding this draft document contact Patricia M. Beers Block 301-827-3340.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)

September 2004
Compliance

Revision 1

Contains Nonbinding Recommendations

Draft — Not for Implementation

Guidance for Industry

Computerized Systems Used in Clinical Trials

Additional copies are available at:

http://www.fda.gov/cder/guidance/index.htm
or
http://www.fda.gov/cber/guidelines.htm
or
http://www.fda.gov/cvm/guidance/guidance.html
or
http://www.fda.gov/cdrh/ggpmain.html
or
http://www.cfsan.fda.gov/~dms/guidance.html
or
http://www.fda.gov/ora/compliance_ref/bimo
or
http://www.fda.gov/oc/gcp

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)

September 2004
Compliance

Revision 1

TABLE OF CONTENTS

Guidance for Industry[1]
Computerized Systems Used in Clinical Trials

This draft guidance, when finalized, will represent the Food and Drug Administration's (FDA's) current thinking on this topic. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. You can use an alternative approach if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach, contact the FDA staff responsible for implementing this guidance. If you cannot identify the appropriate FDA staff, call the appropriate number listed on the title page of this guidance.

I. INTRODUCTION

This document provides guidance about computerized systems that are used to create, modify, maintain, archive, retrieve, or transmit clinical data required to be maintained and/or submitted to the Food and Drug Administration (FDA) These data form the basis for the Agency's decisions regarding the safety and effectiveness of new human and animal drugs, biological products, medical devices, and certain food and color additives. Because the data have broad public health significance, they are expected to be of the highest quality and integrity. This guidance document addresses long-standing FDA regulations concerning clinical trial records. It also addresses requirements of the Electronic Records/Electronic Signatures rule (21 CFR part 11).[2]

Once finalized, this document will supersede the guidance of the same name issued in April 1999. Revisions will make it consistent with Agency policy as reflected in the guidance for industry on *Part 11, Electronic Records; Electronic Signatures — Scope and Application*, which issued in August 2003, and the Agency's international harmonization efforts.[3]

[1] This guidance has been prepared by an Agency working group representing the Bioresearch Monitoring Program Managers for each Center within the Food and Drug Administration, the Office of Regulatory Affairs, and the Office of the Commissioner.

[2] Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations. Part 11 also applies to electronic records submitted to the Agency under the requirements of Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in Agency regulations.

[3] In August 2003, FDA issued the guidance for industry entitled *Part 11, Electronic Records; Electronic Signatures-Scope and Application* clarifying that the Agency intended to interpret the scope of part 11 narrowly and to exercise enforcement discretion with regard to part 11 requirements for validation, audit trails, record retention, and record copying. In 1996, the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) issued *E6 Good Clinical Practice: Consolidated Guidance*.

FDA's guidance documents, including this guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.

II. BACKGROUND

FDA has the authority to inspect all records relating to clinical investigations conducted under 21 CFR 312, 511.1(b), and 812 , regardless of how they were created or maintained (e.g., §§ 312.58, 312.68, and 812.145). FDA established the Bioresearch Monitoring (BIMO) Program of inspections and audits to monitor the conduct and reporting of clinical trials to ensure that supporting data from these trials meet the highest standards of quality and integrity, and conform to FDA's regulations. FDA's acceptance of data from clinical trials for decision-making purposes depends on FDA's ability to verify the quality and integrity of the data during FDA on-site inspections and audits. To be acceptable, the data should meet certain fundamental elements of quality whether collected or recorded electronically or on paper. For example, data should be attributable, legible, contemporaneous, original[4] and accurate.

This guidance addresses how Agency expectations and regulatory requirements regarding data quality might be satisfied where computerized systems are being used to create, modify, maintain, archive, retrieve, or transmit clinical data. Although the primary focus of this guidance is on computerized systems used at clinical sites to collect data, the principles set forth may also be appropriate for computerized systems belonging to contract research organizations, data management centers, and sponsors. Persons using the data from computerized systems should have confidence that the data are no less reliable than data in paper form.

Computerized medical devices, diagnostic laboratory instruments, and instruments in analytical laboratories that are used in clinical trials are not the subject of this guidance. This guidance does not address electronic submissions or methods of their transmission to the Agency, except to the degree to which these records comply with Part 11.

The principles in this guidance may be applied where supporting data or source documents[5] are created (1) in hardcopy and later entered into a computerized system, (2) by direct entry by a human into a computerized system, and (3) automatically by a computerized system.

[4] FDA is allowing original documents to be replaced by certified copies provided the copies are identical and have been verified as such. (see FDA Compliance Policy Guide # 7130.13). See “Definitions” section for a definition of original data.

[5] Under 21 CFR 312.62 (b) reference is made to records that are part of case histories as “supporting data;” the ICH *E6 Good Clinical Practice* consolidated guidance uses the term "source documents." These terms describe the same information and have been used interchangeably in this guidance.

III. GENERAL PRINCIPLES

The Agency recommends the following general principles with regard to computerized systems that are used to create, modify, maintain, archive, retrieve, or transmit clinical data required to be maintained and/or submitted to FDA.

1. We recommend that each study protocol identify at which steps a computerized system will be used to create, modify, maintain, archive, retrieve, or transmit data.

2. For each study, we recommend that documentation identify what software and hardware are to be used in computerized systems that create, modify, maintain, archive, retrieve, or transmit data. We also recommend that this documentation be retained as part of the study records.

3. We recommend that computerized systems be designed (1) so that all requirements assigned to these systems in a study protocol are satisfied (e.g., data are recorded in metric units, the study blinded) and (2) to preclude errors in data creation, modification, maintenance, archiving, retrieval, or transmission.

4. It is important to design a computerized system in such a manner so that all applicable regulatory requirements for record keeping and record retention in clinical trials are met with the same degree of confidence as is provided with paper systems.

5. Under 21 CFR 312.62 , 511.1(b)(7)(ii) and 812.140, the clinical investigator must retain records required to be maintained under part 312, § 511.1(b) and § 812, respectively, for a period of time specified in these regulations. Retaining the original source document or a certified copy of the source document at the site where the investigation was conducted can assist in meeting these regulatory requirements. It can also assist in the reconstruction and evaluation of the trial throughout and after the completion of the trial.

6. When original observations are entered directly into a computerized system, the electronic record is the source document.

   [This guidance seems to clarify that it is the electronic record that is the source document, not the computerized system used to act on the record. (ref: definition of Electronic Record in this document, line 548). We are satisfied, therefore, that the guidance clarifies some past confusion as to whether the source document was the e-record or was the material substrate in a system on which the e-record had been recorded.]

7. Records relating to an investigation must be adequate and accurate in the case of investigational new drug applications (INDs) (see § 312.57 and § 312.62), complete in the case of new animal drugs for investigational use (INADs) (see §511.1(b)(7)(ii)), and accurate, complete and current in the case of investigational device exemptions (IDEs) (see § 812.140(a) and § 812.140(b)). An audit trail that is electronic or consists of other physical, logical, or procedural security measures to ensure that only authorized additions, deletions, or alterations of information in the electronic record have occurred may be needed to facilitate compliance with applicable records regulations. Firms should determine and document the need for audit trails based on a risk assessment that takes into consideration circumstances surrounding system use, the likelihood that information might be compromised, and any system vulnerabilities. We recommend that audit [trails]

Deleted:

Inserted:

Deleted: trials

or other security methods used to capture electronic record activities document who made the changes, when, and why changes were made to the electronic record.

8. We recommend that data be retrievable in such a fashion that all information regarding each individual subject in a study is attributable to that subject.

9. To ensure the authenticity and integrity of electronic records, it is important that security measures be in place to prevent unauthorized access to the data in the electronic record and to the computerized system.

IV. OVERALL APPROACH TO MEETING PART 11 REQUIREMENTS

As described in the FDA guidance entitled *Part 11, Electronic Records; Electronic Signatures-Scope and Application* (August 2003), while the re-examination of part 11 is underway, FDA intends to exercise enforcement discretion with respect to part 11 requirements for validation, audit trail, record retention, and record copying. That is, FDA does not intend to take enforcement action to enforce compliance with these requirements of part 11 while the agency re-examines part 11. Note that part 11 remains in effect and that the exercise of enforcement discretion applies only to the extent identified in the FDA guidance on part 11. Also, records must still be maintained or submitted in accordance with the underlying requirements set forth in the Federal Food, Drug, and Cosmetic Act (Act), the Public Health Service Act (PHS Act), and FDA regulations (other than part 11), which are referred to in this guidance document as *predicate rules*, and FDA can take regulatory action for noncompliance with such predicate rules.[6]

Specific details about the Agency's approach to enforcing part 11 can be found in the *Part 11 Scope and Application* guidance.

V. STANDARD OPERATING PROCEDURES

We recommend that standard operating procedures (SOPs) or other suitable documentation pertinent to the use of the computerized system at the site be available on site.

1. [Where a computerized system is to be used by trial subjects at their homes, it could be construed from the original wording in the draft guidance that the "site" could mean the study subject's home. Since the study subjects are managed from the Investigator site, it should be stated as sufficient to have these SOPs available at the Investigator site and not at the subject's home.]
2. [Such on-site documentation should include:
   - Operating instructions for the system including log on procedures, data entry, electronic signatures (where applicable), backup procedures and access to help and support.

Formatted: Bullets and Numbering

[6] This term refers to underlying requirements set forth in the Federal Food, Drug, and Cosmetic Act, the PHS Act, and FDA regulations (other than 21 CFR Part 11). Regulations governing good clinical practice and human subject protection can be found at 21 CFR parts 50, 56, 312, 511, and 812. See Definitions section at the end of this document listing definitions of this and other terms used in this guidance.

- Policy and procedure on electronic records and electronic signatures (including avoidance of password sharing, time-out, and log off when leaving station)
- A description of how the system to be used by the site allows the site to fulfill the requirements of the investigator under 21CFR312.62.]

[Suggested added text: "We recommend that SOPs be established for the following (and that where such SOP's are maintained by a technology provider, that they be capable of being readily provided onsite on request):]

- System Setup/Installation
- Data Collection and Handling
- System Maintenance
- Data Backup, Recovery, and Contingency Plans
- Security
- Change Control
- Alternative Recording Methods (in the case of system unavailability)

[While we agree that such SOPs need to be made available at the clinical site in case of audit or FDA review, we believe that many modern systems are delivered as networked applications where much of the system operation occurs centrally (offsite). In such cases it seems appropriate for the full system and process documentation to be maintained centrally and made available on site in the event of an audit.]

VI. DATA ENTRY

A. Computer Access Controls

To ensure that individuals have the authority to proceed with data entry, data entry systems must be designed to limit access so that only authorized individuals are able to input data (§ 11.10(d)).[7] Examples of methods for controlling access include using combined identification codes/passwords, physical or electronic tokens or keys, and/or biometric-based identification at the start of a data entry session. Controls and procedures must be in place that are designed to ensure the authenticity and integrity of electronic records created, modified, maintained, or transmitted using the data entry system (§ 11.10). Therefore, we recommend that each user of the system have an individual account into which the user logs-in at the beginning of a data entry session, inputs information (including changes) on the electronic record, and logs out at the completion of data entry session.

We recommend that individuals work only under their own password or other access key and not share these with others. We recommend that individuals not be allowed to log onto the system to provide another person access to the system. We also recommend that passwords or other access keys be changed at established intervals.

[7] As FDA announced in the *Part 11 Scope and Application* guidance, we intend to enforce certain controls for closed systems in § 11.10, including §11.10(d).

1. [We believe that the "accces key" should be clarified to refer either logical OR physical keys such as a card or other electronic "token" bearing or generating an identification code unique to the user (§11.300 (c,d,e)).]
2. [Furthermore, in the case where the study patients may be entering information about themselves, or for any users with physical disabilities, a system making use of a common access code coupled with a unique token or device should also be included in any list of recommended methods of attribution and authorization. Common access codes in conjunction with unique physical devices assigned to each patient simplify operation of the data capture system during conduct of a trial where data is captured directly from patients. In particular, the common code is easier for sites to support without compromising patient privacy. When investigative sites manage patient-specific access codes, the site burden of support increases substantially, simply to help patients who forget their access code and who must each then be led through a secure process to obtain a new access code. Reducing this burden by incorporating physical tokens has been a useful and secure approach in our experience.]
3. [Regulations require that digital signatures (comprised of an ID that can be publicly known and a password that is known only to the user) must be unique. Thus such "signatures" are often used also as "access controls" to provide access to EDC systems for users who will review data as well as those who may act upon trial records in other ways (edit, approve, reject, comment, etc). We understand that FDA has been concerned over the possibility that over time a password may become compromised (used by another person), and therefore FDA required (21 CFR 11.300 (b)) that digital signatures based on identification codes in combination with passwords be "periodically checked, recalled or revised". Many EDC systems thus require periodic changing of passwords. Ironically, however, it appears from interviews with users of such systems that the burden of memorizing and remembering numerous passwords is great enough that many users either write down passwords or work out a system that allows them easily to change to a new version of a familiar password at each change interval. Such habits clearly thwart the intention of the provision.

   An alternative approach, called the forever password, may therefore be worth promoting. The idea is that by supporting "checking" (21CFR§11.300(b) of all uses of a signature, possibly by providing a summary similar to the ones generated by credit card companies, users of an EDC system could inspect all actions undertaken under a particular signature. Users could receive such a summary regularly and check for any un-remembered or inappropriate uses that might indicate that the password had become compromised. The benefit of such a system is that an individual could invest the energy to think up a truly proper password and protect it carefully from disclosure so as to avoid the necessity and work of changing it.]

Formatted: Bullets and Numbering

When someone leaves a workstation, we recommend that the SOP require that person to log off the system. Alternatively, an automatic log off may be appropriate for long idle periods. For short periods of inactivity, we recommend that some kind of automatic protection be installed against unauthorized data entry. An example could be an automatic screen saver that prevents data entry until a password is entered.

B. Audit Trails or other Security Measures

Section 11.10(e) requires persons who use electronic record systems to maintain an audit trail as one of the procedures to protect the authenticity, integrity, and, when appropriate, the confidentiality of electronic records. As clarified in the *Part 11 Scope and Application* guidance, however, the Agency intends to exercise enforcement discretion regarding specific part 11 requirements related to computer-generated, time-stamped audit trails (§ 11.10(e), (k)(2) and any corresponding requirement in § 11.30). Persons must still comply with all applicable predicate rule requirements for clinical trials, including, for example, that records related to the conduct of the study must be adequate and accurate (§§ 312.57, 312.62, and 812.140). It is therefore important to keep track of all changes made to information in the electronic records that document activities related to the conduct of the trial. Computer-generated, time-stamped audit trails or information related to the creation, modification, or deletion of electronic records may be useful to ensure compliance with the appropriate predicate rule.

In addition, clinical investigators must, upon request by FDA, at reasonable times, permit agency employees to have access to, and copy and verify any required records or reports made by the investigator (§§ 312.68, 511.1(b)(7)(ii) and 812.145). In order for the Agency to review and copy this information, FDA personnel should be able to review audit trails or other documents that track electronic record activities both at the study site and at any other location where associated electronic study records are maintained. To enable FDA's review, information about the creation, modification, or deletion of electronic records should be created incrementally, and in chronological order. To facilitate FDA's inspection of this information, we recommend that clinical investigators retain either the original or a certified copy of any documentation created to track electronic records activities.

Even if there are no applicable predicate rule requirements, it may be important to have computer-generated, time-stamped audit trails or other physical, logical, or procedural security measures to ensure the trustworthiness and reliability of electronic records. We recommend that any decision on whether to apply computer-generated audit trails or other appropriate security measures be based on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on data quality and record integrity. Firms should determine and document the need for audit trails based on a risk assessment that takes into consideration circumstances surrounding system use, the likelihood that information might be compromised, and any system vulnerabilities.

If you determine that audit trails or other appropriate security measures are needed to ensure electronic record integrity, we recommend that personnel who create, modify, or delete electronic records not be able to modify the documents or security measures used to track electronic record changes. We recommend that audit trials or other security methods used to capture electronic record activities document who made the changes, when, and why changes were made to the electronic record.

Some examples of methods for tracking changes to electronic records include:

- Computer-generated, time-stamped electronic audit trails.

- Signed and dated printed versions of electronic records that identify what, when, and by whom changes were made to the electronic record. When using this method, it is important that appropriate controls be utilized that ensure the accuracy of these records (e.g., sight verification that the printed version accurately captures all of the changes made to the electronic record).
- Signed and dated printed standard electronic file formatted versions (e.g., pdf, xml or sgml) of electronic records that identify what, when, and by whom changes were made to the electronic record.
- Procedural controls that preclude unauthorized personnel from creating, modifying, or deleting electronic records or the data contained therein.

C. Date/Time Stamps

We recommend that controls be put in place to ensure that the system's date and time are correct. The ability to change the date or time should be limited to authorized personnel and such personnel should be notified if a system date or time discrepancy is detected. We recommend that someone always document changes to date or time. We do not expect documentation of time changes that systems make automatically to adjust to daylight savings time conventions.

We also recommend that dates and times include the year, month, day, hour, and minute. The Agency encourages establishments to synchronize systems to the date and time provided by trusted third parties.

Clinical study computerized systems are likely be used in multi-center trials and may be located in different time zones. For systems that span different time zones, it is better to implement time stamps with a clear understanding of the time zone reference used. We recommend that system documentation explain time zone references as well as zone acronyms or other naming conventions.

VII. SYSTEM FEATURES

The Agency recommends that a number of computerized system features be available to facilitate the collection, inspection, review, and retrieval of quality clinical data. Key features are described here.

A. Systems Used for Direct Entry of Data

We recommend that prompts, flags, or other help features be incorporated into the computerized system to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range. We recommend against the use of features that automatically enter data into a field when the field is bypassed.

B. Retrieval of Data and Record Retention

FDA expects to be able to reconstruct a clinical study submitted to the agency. This means that documentation, such as that described in the General Principles, Sections III.1, III.2 and III.5, should fully describe and explain how data were obtained and managed and how electronic records were used to capture data. We suggest that your decision on how to maintain records be based on predicate rule requirements and that this documented decision be based on a justified risk assessment and a determination of the value of the records over time. As explained in the Part 11 Scope and Application guidance, FDA does not intend to object to required records that are archived in electronic format; nonelectronic media such as microfilm, microfiche, and paper; or to a standard electronic file format (such as PDF, XML, or SGML). Persons must still comply with all predicate rule requirements, and the records themselves and any copies of required records should preserve their original content and meaning. Paper and electronic record and signature components can co-exist (i.e., as a hybrid system) as long as the predicate requirements (21 CFR parts 50, 56, 312, 511, and 812) are met, and the content and meaning of those records are preserved.

It is not necessary to reprocess data from a study that can be fully reconstructed from available documentation. Therefore, actual application software, operation systems, and software development tools involved in processing of data or records do not need to be retained.

VIII. SYSTEM SECURITY

In addition to internal safeguards built into the computerized system, external safeguards should be put in place to ensure that access to the computerized system and to the data is restricted to authorized personnel as required by 21 CFR 11.10(d). We recommend that staff be kept thoroughly aware of system security measures and the importance of limiting access to authorized personnel.

SOPs should be developed and implemented for handling and storing the system to prevent unauthorized access. Controlling system access can be accomplished through the following provisions of part 11 that, as discussed in the part 11 guidance, FDA intends to continue to enforce:

- Operational system checks (§ 11.10(f));
- Authority checks (§ 11.10(g));
- Device (e.g., terminal) checks (§ 11.10(h)); and
- The establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures (§ 11.10(j)).

The Agency recommends that access to data be restricted and monitored through the system's software with its required log-on, security procedures, and audit trail (or other selected security measures to track electronic record activities). We recommend that procedures and controls be implemented to prevent the data from being altered, browsed, queried, or reported via external software applications that do not enter through the protective system software.

We recommend that a cumulative record be available that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. We recommend that the record be kept in the study documentation, accessible at the site.

> [Where patients are authorized to enter data pertaining to themselves into the system (and thus have privileges on the system), we suggest that this provision specifically exclude patients so as to protect their privacy. Usually all patient privileges are identical and the objective of this recommendation can be met without disclosing the patient names by using codes and processes that protect confidentiality. Also, we recommend that, except under audit or FDA review, investigator sites should have ready access to their own information concerning access rights and privileges, but should not routinely have access to such information about users from other investigator sites.]

If a sponsor supplies computerized systems exclusively for clinical trials, we recommend that the systems remain dedicated to the purpose for which they were intended and validated. If a computerized system being used for a clinical study is part of a system normally used for other purposes, we recommend that efforts be made to ensure that the study software be logically and physically isolated as necessary to preclude unintended interaction with nonstudy software. If any of the software programs are changed, we recommend that the system be evaluated to determine the effect of the changes on logical security.

We recommend that controls be implemented to prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software.

IX. SYSTEM DEPENDABILITY

The Agency recommends that sponsors ensure and document that all computerized systems conform to their own established requirements for completeness, accuracy, reliability, and consistent intended performance.

We recommend that systems documentation be readily available at the investigator site where clinical trials are conducted and provide an overall description of the computerized systems and the relationships among hardware, software, and physical environment.

As noted in the *Part 11 Scope and Application* guidance, the Agency intends to exercise enforcement discretion regarding specific part 11 requirements for validation of computerized systems. We suggest that your decision to validate computerized systems and the extent of the validation take into account the impact the systems have on your ability to meet predicate rule requirements. You should also consider the impact those systems might have on the accuracy, reliability, integrity, availability, and authenticity of required records and signatures. Even if there is no predicate rule requirement to validate a system, it may still be important to validate the system, based on criticality and risk, to ensure the accuracy, reliability, integrity, availability and authenticity of required records and signatures.

We recommend that you base your approach on a justified and documented risk assessment and determination of the potential of the system to affect data quality and record integrity. For

example, in the case where data are directly entered into electronic records and the business practice is to rely on the electronic record, validation of the computerized system is important. However when a word processor is used to generate SOPs for use at the clinical site, validation would not be important.

If validation is required, FDA may ask to see the documentation that demonstrates computer system validation. The study sponsor is responsible for making any such documentation available if requested at the time of inspection at the site where software is used. Clinical investigators are not generally responsible for validation unless they originated or modified software.

Deleted: regulated company's

Deleted: software

A. Legacy Systems

As noted in the *Part 11 Scope and Application* guidance, the Agency intends to exercise enforcement discretion with respect to all part 11 requirements for systems that otherwise were fully operational prior to August 20, 1997, the effective date of part 11, under the circumstances described below. These systems are also known as legacy systems. The Agency does not intend to take enforcement action to enforce compliance with any part 11 requirements if all the following criteria are met for a specific system:

- The system was in operation before the part 11 effective date.
- The system met all applicable predicate rule requirements prior to the part 11 effective date.
- The system currently meets all applicable predicate rule requirements.
- There is documented evidence and justification that the system is fit for its intended use.

If a system has changed since August 20, 1997, and if the changes would prevent the system from meeting predicate rule requirements, part 11 controls should be applied to part 11 records and signatures pursuant to the enforcement policy expressed in the part 11 guidance. Please refer to the *Part 11 Scope and Application* guidance for further information.

B. Off-the-Shelf Software [Need a definition for "Off-the-Shelf Software"]

While the Agency has announced that it intends to exercise enforcement discretion regarding specific part 11 requirements for validation of computerized systems, persons must still comply with all predicate rule requirements for validation. We suggested in the guidance for industry on part 11 that the impact of computerized systems on the accuracy, reliability, integrity, availability, and authenticity of required records and signatures be considered when you decide whether to validate, and noted that even absent a predicate rule requirement to validate a system, it might still be important to validate in some instances.

For most off-the-shelf software, the design level validation will have already been done by the company that wrote the software. Given the importance of ensuring valid clinical trial data, FDA suggests that the sponsor or contract research organization (CRO) have documentation (either original validation documents or on-site vendor audit documents) of this design level validation by the vendor and would itself have performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections. Detailed

documentation of any additional validation efforts performed by the sponsor or CRO will preserve the findings of these efforts.

In the special case of software and systems that are: (1) purchased off-the-shelf, (2) designed for and widely used for general purposes, and (3) unmodified, the sponsor or contract research organization may not have access to the supplier's validation documentation. FDA suggests that the sponsor or contract research organization perform sufficient validation (e.g., by use of test data sets) and research known software limitations, problems, and defect corrections) to document that the software or system is qualified to perform its intended use in the clinical trial.

Deleted: of database and spreadsheet

Deleted: is

Deleted: , and (4) not being used for direct entry of data

Deleted: to documentation

Deleted: of design level

Deleted: functional testing

Deleted: .

In the case of off-the-shelf software or systems, we recommend that the following be available to the Agency on request :

- A written design specification that describes what the software or system is intended to do and how it is intended to do it within the context of the clinical trial;
- A written test plan based on the design specification, including both structural and functional analysis; and
- Test results and an evaluation of how these results demonstrate that the predetermined design specification has been met.

Additional guidance on general software validation principles can be found in FDA's guidance entitled *General Principles of Software Validation; Final Guidance for Industry and FDA Staff*.

C. Change Control

FDA recommends that written procedures be put in place to ensure that changes to the computerized system, such as software upgrades, including security and performance patches, equipment, or component replacement, or new instrumentation, will maintain the integrity of the data and the integrity of protocols. We recommend that the effects of any changes to the system be evaluated and a decision made regarding whether, and if so, what level of validation activities related to those changes would be appropriate. We recommend that validation be performed for those types of changes that exceed previously established operational limits or design specifications. Finally, we recommend that all changes to the system be documented.

X. SYSTEM CONTROLS

The Agency recommends that appropriate system control measures be developed and implemented.

- Software Version Control

We recommend that measures be put in place to ensure that versions of software used to generate, collect, maintain, and transmit data are the versions that are stated in the systems documentation.

- Contingency Plans

We recommend that written procedures describe contingency plans for continuing the study by alternate means in the event of failure of the computerized system.

- Backup and Recovery of Electronic Records

When electronic formats are the only ones used to create and preserve electronic records, the Agency recommends that backup and recovery procedures be outlined clearly in SOPs and be sufficient to protect against data loss. We also recommend that records be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data. We recommend that records be stored at a secure location specified in the SOPs. Storage is typically offsite or in a building separate from the original records.

We recommend that backup and recovery logs be maintained to facilitate an assessment of the nature and scope of data loss resulting from a system failure.

Firms that rely on electronic and paper systems should determine the extent to which backup and recovery procedures are needed based on the need to meet predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on data quality and record integrity.

XI. TRAINING OF PERSONNEL

Under 21 CFR 11.10(i), firms using computerized systems must determine that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks.

The Agency recommends that training be provided to individuals in the specific operations with regard to computerized systems that they are to perform. We recommend that training be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerized system and with any changes to the system during the course of the study.

We recommend that employee education, training, and experience be documented.

XII. COPIES OF RECORDS AND RECORD INSPECTION

FDA has the authority to inspect all records relating to clinical investigations conducted under 21 CFR Parts 312 and 812, regardless of how the records were created or maintained (21 CFR 312.58, 312.68, and 812.145). Therefore, you should provide the FDA investigator with reasonable and useful access to records during an FDA inspection. As noted in the *Part 11, Electronic Records; Electronic Signatures- Scope and Application* guidance, the Agency intends to exercise enforcement discretion with regard to specific part 11 requirements for generating

copies of records (§ 11.10(b) and any corresponding requirement in § 11.30). We recommend that you supply copies of electronic records by:

- Producing copies of records held in common portable formats when records are maintained in these formats
- Using established automated conversion or export methods, where available, to make copies available in a more common format (e.g., pdf, xml, or sgml formats)

Regardless of the method used to produce copies of electronic records, it is important that the copying process used produces copies that preserve the content and meaning of the record. For example, if you have the ability to search, sort, or trend records, copies given to FDA should provide the same capability if it is reasonable and technically feasible. FDA expects to inspect, review, and copy records in a human readable form at your site, using your hardware and following your established procedures and techniques for accessing records.

We recommend you contact the Agency if there is any doubt about what file formats and media the Agency can read and copy.

XIII. CERTIFICATION OF ELECTRONIC SIGNATURES

As required by 21 CFR 11.100(c), persons using electronic signatures to meet an FDA signature requirement must, prior to or at the time of such use, certify to the Agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

As set forth in § 11.100(c)(1), the certification must be submitted in paper, signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, Maryland 20857. The certification is to be submitted prior to or at the time electronic signatures are used. However, a single certification can be used to cover all electronic signatures used by persons in a given organization. This certification is created by persons to acknowledge that their electronic signatures have the same legal significance as their traditional handwritten signatures. See the following example of a certification statement:

> Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that ___[*name of organization*]__ intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures.

[We have wondered whether the Agency has considered the case where patients may be entering information and then using an electronic signature to confirm authorship or other possible actions on electronic records. The certification statement as written does not appear to apply to patients in a trial since they are not employees, agents or representatives of either the sponsor, the site, or the technology providers involved with the trial. This gap would compel a substantial administrative burden in a trial where use of electronic

signatures by patients might be contemplated since each patient would have to file an intention to use an electronic signature with the FDA. We do not think the Agency intended to create such a burden or to thereby forestall the possibility of developing systems in which electronic signatures might realistically be employed by patients participating in a trial.]

DEFINITIONS

The following is a list of definitions for terms as they are used in, and for the purposes of, this guidance document.

Attributable Data: Attributable data are those that can be traced to individuals responsible for observing and recording the data. In an automated system, attributability could be achieved by a computer system designed to identify individuals responsible for any input.
[Where subjects or family members entitled to confidentiality may be entering data or otherwise acting on electronic records in a clinical trial, it is important that the automated system support attributability, but do so in a way that preserves confidentiality. We note, parenthetically, that the HIPAA and Part 11 requirements seem to be at odds—HIPAA emphasizing privacy and Part 11 emphasizing attributability and, for any signature manifestation, full disclosure of identity by printed name. We have sought to limit the disclosure of patient attributability for data entered directly by patients or families so that only the personnel at the investigative site can review such data with full attribution immediately visible on the electronic record. However, this is an area of ongoing concern by sponsors who must collect attributable information and also protect privacy. The Agency may wish either to address this concern or provide more explicit guidance]

Audit Trail: An *audit trail* is a secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record.

Certified Copy: A copy of original information that has been verified, as indicated by dated signature, as an exact copy having all of the same attributes and information as the original

Computerized System: A *computerized system* includes computer hardware, software, and associated documents (e.g., user manual) that create, modify, maintain, archive, retrieve, or transmit in digital form information related to the conduct of a clinical trial.

Direct Entry: Recording data where an electronic record is the original capture of the data. Examples are the keying by an individual of original observations into the system, or automatic recording by the system of the output of a balance that measures subject's body weight.

Electronic Record: Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Signature: A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

eSource: Source data captured initially into a permanent electronic record. (CDISC) NOTE: "Permanent" in the context of these definitions implies that any changes made to the electronic data are recorded via an audit trail. See source data. [ICH E3]

[1. We recognize that the Agency has thought carefully about the distinction between a record and the physical substrate used to capture the information in a record. We note that eSource records can be migrated, copied, and multiply stored using validated processes and all be absolutely identical in informational content. Each and all such records are (or ought to be able to be construed as) eSource in a trial.
2. We recommend that the guidance include a comment on the distinction between a migrated or automatically copied record in a validated system to make such migrations or copies properly and a "certified copy", which is a copy that has been manually certified to be identical to an original record.]

Original data: *Original data* are those values that represent the first recording of study data. FDA is allowing original documents and the original data recorded on those documents to be replaced by certified copies provided the copies are identical and have been verified as such. (see FDA Compliance Policy Guide # 7150.13

Deleted: 7130

[We recommend caution concerning the notion that original data are a "first" to occur record. ICH E6 supports the concept that the source document be specified for a trial [6.4.9]. The preamble to Part 11 also includes the example of an EKG device simultaneously recording an electronic and paper EKG—either the electronic or the paper record *could be* the source, but which one actually is intended to serve as the source document for the trial should be specified. The preamble indicates that the specification should be based on which record is to be used in an ongoing sense in the clinical trial (and would thus be the one to show any corrections and changes). We think the source document for a trial should be the original document containing the data that is to be used in the study, not simply the first capture of that information. For example, a birthdate might be lodged in a hospital or site record system, but the source for the field in a CRF might well be a paper or electronic source entry done during an interview to qualify the subject for the trial.]

Predicate rule: This term refers to underlying requirements set forth in the Federal Food, Drug, and Cosmetic Act, the PHS Act, and FDA regulations (other than 21 CFR part 11). Regulations governing good clinical practice and human subject protection can be found at 21 CFR parts 50, 56, 312, 511, and 812.

Software Validation: Confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses and that the particular requirements implemented through the software can be consistently fulfilled. *Design level validation* is that portion of the software validation that takes place in parts of the software life cycle before the software is delivered to the end user.

Source Documents: Original documents and records including, but not limited to, hospital records, clinical and office charts, laboratory notes, memoranda, subjects' diaries or evaluation checklists, pharmacy dispensing records, recorded data from automated instruments, copies or transcriptions certified after verification as being accurate and complete, microfiches, photographic negatives, microfilm or magnetic media, x-rays, subject files, and records kept at

the pharmacy, at the laboratories, and at medico-technical departments involved in the clinical trial.

Transmit: *Transmit* is to transfer data within or among clinical study sites, contract research organizations, data management centers, or sponsors. Other Agency guidance covers transmission from sponsors to the Agency.

REFERENCES

FDA, *21 CFR Part 11,* "Electronic Records; Electronic Signatures; Final Rule." *Federal Register* Vol. 62, No. 54, 13429, March 20, 1997.

FDA, *Compliance Program Guidance Manual*, "Compliance Program 7348.810 - Sponsors, Contract Research Organizations and Monitors," October 30, 1998.

FDA, *Compliance Program Guidance Manual*, "Compliance Program 7348.811 - Bioresearch Monitoring - Clinical Investigators," September 2, 1998.

FDA, *Glossary of Computerized System and Software Development Terminology*, 1995.

FDA, *Good Clinical Practice VICH GL9*, 2001.

FDA, *Guideline for the Monitoring of Clinical Investigations*, 1988.

FDA, *Information Sheets for Institutional Review Boards and Clinical Investigators*, 1998.

FDA, *Software Development Activities*, 1987.

International Conference on Harmonisation, "E6 Good Clinical Practice: Consolidated Guideline," *Federal Register*, Vol. 62, No. 90, 25711, May 9, 1997.

FDA, *Part 11, Electronic Records; Electronic Signatures — Scope and Application*, 2003.

FDA, *General Principles of Software Validation; Guidance for Industry and FDA Staff*, 2002.